Sincronização de identidade do Cisco Secure Access com Ative Diretory e Microsoft EntraID

Contents

Problema

Os usuários experimentaram desafios ao tentar provisionar usuários e grupos de duas origens de identidade com o mesmo nome de domínio no Cisco Secure Access. O cenário específico envolvia a sincronização de identidades do Ative Diretory local e do Microsoft EntraID (antigo Azure AD), em que ambas as fontes usavam o mesmo nome de domínio (por exemplo, domain.com).

As principais preocupações foram:

- Entendendo como a propriedade de identidade e o mapeamento de associação de grupo se comportam quando os mesmos usuários e grupos existem em ambas as origens de identidade
- Garantir a aplicação consistente da política de acesso seguro para usuários híbridos que acessam recursos no local e na nuvem
- Manter a visibilidade de IP interna para usuários nessa configuração de identidade híbrida
- Determinar se a sincronização simultânea de ambas as origens causaria problemas em um ambiente de produção

A documentação indicou que "a sincronização simultânea dos mesmos usuários e grupos do Cisco AD Connector e do aplicativo Cisco User Management for Secure Access não é suportada e leva à imposição de regras de acesso inconsistentes".

Ambiente

- Cisco Secure Access com conector AD e integração EntraID

- Ative Diretory local com nome de domínio correspondente ao domínio EntraID
- Microsoft EntraID (Azure AD) com o mesmo nome de domínio do AD local
- Configuração de SAML SSO para federação de identidade
- Módulo Secure Web Gateway (SWG) para aplicação de políticas
- Ambiente híbrido que exige acesso a recursos locais e em nuvem

Resolução

O seguinte comportamento foi confirmado para sincronização simultânea das origens do Ative Diretory e do EntraID:

Comportamento de Sincronização de Grupo

Ao sincronizar grupos com o mesmo nome de ambas as origens:

- Dois objetos de grupo separados são criados no Cisco Secure Access - um de cada origem
- Os grupos podem ser diferenciados por seu prefixo de origem em políticas de acesso
- Os grupos locais do AD aparecem como: AD-Domain/GroupName
- Os grupos EntraID aparecem como: Nome do grupo

A verificação do laboratório mostrou uma sincronização bem-sucedida com a mensagem "Êxito. <<<< Sincronizado" para grupos de vários domínios EntraID.

Comportamento da Sincronização do Usuário

Ao sincronizar usuários com a mesma ID de usuário de ambas as origens:

- A identidade do usuário é substituída durante a sincronização

- Apenas uma ID de usuário exclusiva permanece visível no Secure Access
- A origem de sincronização final determina os atributos do usuário e as associações do grupo
- A sincronização de EntraID normalmente tem precedência sobre o AD local quando ambos são configurados

Configuração da política de acesso

Os dois tipos de grupo podem ser utilizados em políticas de acesso:

- Faça referência a grupos locais do AD usando o caminho completo: AD-Domain/GroupName
- Faça referência a grupos EntraID usando o nome simples: Nome do grupo
- As políticas podem diferenciar os usuários com base em sua origem de associação de grupo

Seguir a configuração funciona bem para muitos clientes.

```
1    Only provision identities from on-prem AD - for VA DNS protection
2    Use Azure entra for SSO/user authentication (no identities to be provisioned from Azure) - for SWG
```

Causa

Durante nosso teste, confirmamos que sempre que um usuário é sincronizado a partir do On-Premises AD Connector, ele efetivamente "reivindica" essa identidade no painel do Umbrella. Se esse mesmo usuário já existir por meio da sincronização do Azure AD, a sincronização Local substituirá os dados de usuário EntraID existentes.

Esse comportamento é uma limitação documentada. De acordo com a documentação técnica oficial da Cisco: https://securitydocs.cisco.com/docs/csa/china/olh/129444.dita

"A sincronização simultânea das mesmas identidades de usuário e grupo do Umbrella AD

Connector e do aplicativo do Cisco Umbrella Azure AD não é suportada e leva à aplicação de política inconsistente."

Conclusão: A configuração desejada (visibilidade de VA para usuários existentes no Azure e no Local) está confirmada como uma configuração sem suporte.O caminho a seguir requer o uso de Clientes Móveis para garantir a aplicação consistente da identidade.

Conteúdo relacionado

- Provisionar Identidades do Azure AD - Documentação do Cisco Umbrella
- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.